PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 28.7.2000

PCT/FI 00 / 00495

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija
Applicant

Nokia Telecommunications Oy
Helsinki

Patenttihakemus nro
Patent application no

991283

Tekemispäivä
Filing date

04.06.1999

Kansainvälinen luokka
International class

H04K

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Keksinnön nimitys
Title of invention

"Autentikaation ja salauksen järjestäminen matkaviestinjärjestelmässä"

Hakijan nimi on hakemusdiaariin **05.12.1999** tehdyn nimenmuutoksen jälkeen **Nokia Networks Oy.**

The application has according to an entry made in the register of patent applications on **05.12.1999** with the name changed into **Nokia Networks Oy.**

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

TARKASTAJA

CERTIFIED COPY OF PRIORITY DOCUMENT

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Autentikaation ja salauksen järjestäminen matkaviestinjärjestelmässä

Keksinnön tausta

Keksinnön kohteena on itsenäisten patenttivaatimusten johdanto-osissa esitetty menetelmä ja järjestelmä tietosuojauksen järjestämiseksi.

Matkaviestinjärjestelmissä on ainakin yhtenä osana siirtotietä langaton osuus, jolloin tiedonsiirto tapahtuu radiotien kautta. Radiotie on fyysisesti avoin resurssi, josta aiheutuu turvallisuusriskejä. Digitaalisissa matkaviestinjärjestelmissä on kehitetty erilaisia ratkaisuja tietosuojauksen järjestämiseksi, esimerkiksi salausmenetelmiä ja käyttäjän tai tilaajan tunnistus- eli autentikaatiomenetelmiä.

Käyttöoikeuden varmistamiseksi matkaviestinjärjestelmissä tyypillisesti matkaviestinverkko suorittaa tilaajan autentikaation. Esimerkiksi digitaalisessa GSM-järjestelmässä matkaviestin käsittää tilaajan tunnistussovelluksen SIM (Subscriber Identity Module), joka käsittää välineet tilaajan autentikoimiseksi. SIM-sovelluksessa käytetään edelleen PIN-tunnuksen (Personal Identity Number) varmistusta, jolloin ainoastaan tunnusluvun tietävä henkilö voi käyttää SIM-sovellusta. Autentikaatiossa matkaviestin välittää GSM-verkolle tunnistetiedot, joiden perusteella SIM ja täten myös tilaaja tunnistetaan. SIM käsittää matkaviestinoperaattorikohtaisia tietoja, mm. matkaviestinpalvelujen tilaajan SIM-kohtaisen tilaajatunnuksen IMSI (International Mobile Subscriber Identity). Tyypillisesti SIM käsittää myös tilapäisen paikallisen alueen (location area) tunnuksen TMSI (Temporary Mobile Subscriber Identity), jonka avulla voidaan välttää IMSI-tunnuksen siirtäminen radiotien yli.

Matkaviestinkeskus MSC (Mobile Switching Center), joka tyypillisesti käsittää myös vierailijarekisterin VLR (Visitor Location Register), välittää autentikaatiopyynnön autentikaatiokeskukselle AuC (Authentication Centre). Autentikaatiokeskus AuC sijaitsee tyypillisesti osana tilaajan kotirekisteriä HLR (Home Location Register). Autentikaatiokeskuksessa säilytetään tilaajan autentikaatiotietoja ja -algoritmeja. Autentikaatiokeskus AuC valitsee autentikaatiopyynnön käsittämän tilaajatunnuksen IMSI perusteella tilaajakohtaisen autentikaatioavaimen Ki. Lisäksi satunnaislukugeneraattori generoi joukon satunnaislukuparametreja RAND, joista yhdessä avaimen Ki kanssa muodostetaan autentikaation algoritmilla A3 tarkistusparametri SRES (Signed Result) jokaiselle RAND-parametrille. Autentikaatiokeskus AuC välittää nämä RAND/SRES-parametrit tyypillisesti samanaikaisesti lasketun salausavaimen Kc ohella vierailijarekisteriin VLR, johon ne tallennetaan.

Kun VLR haluaa autentikoida tilaajan, se valitsee tätä tilaajaa vastaavasta RAND/SRES-taulukosta parametrille RAND-arvon ja välittää sen matkaviestimeen ja edelleen tilaajan tunnistussovellukselle SIM. SIM käsittää saman autentikaatioavaimen Ki ja autentikaatioalgoritmin A3 kuin autentikaatiokeskuksessa AuC käytetyt. SIM laskee vastaanottamaansa RAND-parametrin ja avaimen Ki avulla algoritmia A3 käyttäen SRES-parametrin, joka on matkaviestimen autentikaatiovaste. Matkaviestin palauttaa SRES-parametrin vierailijarekisterille VLR. VLR vertaa matkaviestimen lähettämää SRES-arvoa tallennettuun SRES-arvoon ja jos ne ovat samat, autentikaatio on onnistunut. GSM-verkko voi pyytää autentikaatiota periaatteessa missä tahansa vaiheessa, kun matkaviestin on verkkoon rekisteröityneenä. Autentikaatio voidaan suorittaa erityisesti aina matkaviestimen rekisteröityessä verkkoon.

Salausta käytetään monissa tietoliikennejärjestelmissä estämään siirrettävän tiedon kulkeutuminen väärille tahoille. Esimerkiksi GSM-järjestelmässä on mahdollista käyttää vaikeasti selvitettävää tiedonsiirron salausta, jolloin digitaaliseen muotoon muunnettu puhe ja data salataan (ciphering) matkaviestimessä siirrettäväksi radiotien yli. Vastaavasti GSM-verkossa vastaanotettu salattu lähete muutetaan takaisin salaamattomaksi puheeksi ja dataksi (deciphering). Tämän hakemuksen yhteydessä salaus voi tarkoittaa joko liikenteen salaamista tai salauksen purkamista. Salauksessa ja käyttäjän tunnistamisessa käytetään salausavaimia ja -algoritmeja, jotka ovat edullisesti vain asianomaisten lähetys- ja vastaanottolaitteiden hallussa.

GSM-järjestelmässä matkaviestinkeskuksen MSC/VLR autentikoitua käyttäjän voidaan aloittaa siirrettävän liikenteen salaus. Salausavain Kc lasketaan autentikaation yhteydessä salaisen avaimen Ki ja satunnaisluvun RAND avulla algoritmiä A8 käyttäen sekä autentikaatiokeskuksessa AuC että tilaajan tunnistussovelluksessa SIM. Tyypillisesti algoritmit A3 ja A8 on toteutettu niin, että sekä SRES-parametri että salausavain Kc lasketaan samanaikaisesti. Autentikaatiokeskus välittää autentikaatioparametreissä salausavaimen Kc RAND- ja SRES-parametrien ohella vierailijarekisteriin VLR, jolloin nämä kolme parametriä muodostavat ns. tripletin. Salausavain Kc talletetaan vierailijarekisteriin VLR. Vierailijarekisteri VLR välittää satunnaisluvun RAND SIM-sovellukselle autentikaatiota ja salausavaimen laskemista varten. SIM laskee RAND-parametrin ja salaisen avaimen Ki perusteella algoritmia A8 hyväksikäyttäen salausavaimen Kc tyypillisesti SRES-parametrin laskemisen yhteydessä. Näinollen salausavaimen Kc laskeminen on yksi osa GSM-

autentikaatiota. Salausavain Kc talletetaan SIM-sovellukselle. Kc on GSM-standardin mukaisesti enintään 64 bittiä.

Matkaviestinkeskuksen MSC/VLR määrätessä salauksen aloitettavaksi salausavain Kc välitetään vierailijarekisteristä VLR tukiasemalle. Edelleen välitetään käsky matkaviestimelle, joka ottaa käyttöön tilaajan tunnistusyksikössä SIM lasketun Kc:n. GSM-verkko valitsee salausalgoritmin matkaviestimen välittämän ns. classmark-tunnisteen käsittämän salausalgoritmin tunnisteen perusteella. Tukiasema ja matkaviestin suorittavat liikenteen salauksen ja salauksen purkamisen liikenteen suunnasta riippuen salausavaimen Kc ja liikennekehyksen numeron avulla käyttäen algoritmia A5. GSM-järjestelmän yksityiskohtaisempi kuvaus löytyy esimerkiksi kirjasta "The GSM System for Mobile Communications", M. Mouly and M. Pautet, Palaiseau, France, 1992, ISBN:2-9507190-0-7.

Ns. kolmannen sukupolven matkaviestinjärjestelmiä on kehitetty eri puolilla maailmaa. 3GPP (3rd Generation Partnership Project) standardoi GSM-järjestelmään perustuvaa kolmannen sukupolven matkaviestinjärjestelmää UMTS (Universal Mobile Telecommunications System), jossa on mm. uusi radiorajapinta. UMTS:n radiorajapinta tulee perustumaan WCDMA-tekniikkaan (Wideband Code Division Multiple Access). GSM-ydinverkkoa (core network) tullaan hyödyntämään UMTS-järjestelmässä, jolloin yhteydenhallinta ja liikkuvuudenhallinta tullevat olemaan monelta osin samankaltaisia. UMTS-järjestelmä tulee tarjoamaan piirikytkentäisiä palveluita ja pakettikytkentäisiä palveluita. Pakettikytkentäiset palvelut todennäköisesti pohjautuvat GSM:n GPRS-palveluun (General Packet Radio Service).

Olennaisena vaatimuksena UMTS-järjestelmässä on handovervaatimus GSM:n ja UMTS:n välillä. Handoverilla tarkoitetaan tämän hakemuksen yhteydessä radioliikenneyhteyden ja -vastuun siirtoa käyttäjän palvelulle tarjottavan yhteyden välillä katkeamatta lähdejärjestelmästä kohdejärjestelmään. GSM/UMTS-handoverissa yhteys siis siirtyy UMTS-järjestelmästä GSM-järjestelmään tai päinvastoin. Käyttäjälle tarjottava yhteys pysyy GSM/UMTS handoverissa vastaavalla tavalla katkeamattomana kuin nykyäänkin GSM-järjestelmän sisäisessä handoverissa. Tämä mahdollistaa UMTS-järjestelmän nopean yleistymisen, koska erityisesti alussa voidaan tukeutua GSM-järjestelmän laajaan peittoalueeseen. Tätä tarkoitusta varten on oletettavaa, että markkinoille ilmestyy ainakin sekä GSM- että UMTS-järjestelmää tukevia ns. dual-mode matkaviestimiä.

UMTS-järjestelmän standardointityössä ollaan turvallisuusarkkitehtuurin osalta päätymässä periaatteiltaan GSM:n toimintoja vastaavaan ratkaisuun. Tällöin voidaan saavuttaa mahdollisimman hyvä yhteensopivuus GSM-arkkitehtuurin kanssa. Sekä UMTS-verkko että GSM:n tunnistussovelluksen SIM kaltainen USIM-sovellus (User Service Identity Module) käsittävät salaisen avaimen, jonka autentikaation suorittaminen edellyttää. Muutoksia tulee lähinnä avainten pituuksiin ja käytettäviin algoritmeihin, 3GPP:n dokumentissa TR S3.03 versio 0.1.2 "3G Security: Security Architecture" käsitellään UMTS-järjestelmän turvallisuusvaatimuksia. Erityisesti käytettävä salausavain tullee olemaan pidempi kuin GSM-järjestelmässä.

GSM-järjestelmän tukemiseksi USIM-sovelluksen käsittävä älykortti UICC (UMTS IC Card) voi käsittää myös GSM-järjestelmän tilaajan tunnistussovelluksen SIM. UMTS-järjestelmässä on myös vaatimuksena tarjota palveluita matkaviestimille, joihin on asetettu ainoastaan GSM SIM-tunnistussovelluksen käsittävä älykortti. Edelleen alkuvaiheessa GSM/UMTS-ydinverkko voi olla sama, joten UMTS-järjestelmän ydinverkko voi tukea myös GSM-järjestelmän mukaista autentikaatiota ja salausta.

GSM-järjestelmässä handover-tilanteessa välitetään matkaviestinkeskusten välisessä handoverissa käytössä olevat salausparametrit, kuten salausavain, lähdeverkosta kohdeverkkoon. Tällöin siirrettäessä yhteys GSM-verkosta UMTS-verkkoon voidaan käyttää GSM:n mukaista salausavainta Kc liikenteen pysyessä koko ajan salattuna. Edellytyksenä on luonnollisesti, että UMTS-verkko tukee GSM-järjestelmän mukaista salausta. Mahdollisesti voidaan suorittaa handoverin jälkeen myös UMTS-järjestelmän mukainen autentikaatio ja siirtyä käyttämään UMTS:n salausavainta.

Matkaviestimen ollessa UMTS-verkossa sillä on käytössään UMTS-järjestelmän mukainen salausavain. Ongelmaksi UMTS-järjestelmästä GSM-järjestelmään handoveria tehtäessä muodostuu salaus, sillä GSM-järjestelmän mukainen tukiasemajärjestelmä BSS (Base Station Sub-system) ei välttämättä pysty suorittamaan salausta UMTS-parametreillä. Näin ollen UMTS:n salausavainta ei voida käyttää sellaisenaan GSM:n periaatteiden mukaan handoverin jälkeen. Tunnetun tekniikan mukaisesti GSM-järjestelmään siirryttäessä voidaan handoverin jälkeen suorittaa GSM-järjestelmän mukainen autentikaatio. Tällöin voidaan siirtyä GSM-salaukseen salausavaimen Kc laskemisen jälkeen. Tämä kuitenkin vaatii aikaa ja osa liikenteestä siirtyy salaamattomana GSM-radiorajapinnan yli.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää menetelmä ja menetelmän toteuttava laitteisto siten, että yllä mainitut ongelmat saadaan ratkaistua. Keksinnön tavoitteet saavutetaan menetelmällä ja järjestelmällä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että suoritetaan matkaviestinjärjestelmän, kuten GSM-järjestelmän, mukaisen ns. toisen matkaviestinverkon salausavaimen määrittäminen eri matkaviestinjärjestelmän, kuten UMTS-järjestelmän, mukaisessa ensimmäisessä matkaviestinverkossa matkaviestimen toimiessa ensimmäisessä matkaviestinverkossa. Tällöin voidaan määrittää toisen matkaviestinverkon mukainen ns. toinen salausavain, joka voidaan edullisesti tallettaa sekä matkaviestimeen että pääsääntöisesti ns. ensimmäistä salausavainta liikenteen salaukseen käyttävään ensimmäiseen matkaviestinverkkoon. Näin saavutetaan se etu, että toisen matkaviestinverkon, kuten GSM-verkon, mukainen toinen salausavain on valmiina jo ennen mahdollista handover-tilannetta.

Handover-tilanteessa ensimmäisestä matkaviestinverkosta voidaan välittää toinen salausavain salauksen suorittavalle verkkoelementille, kuten tukiasemalle, toisessa matkaviestinverkossa. Edelleen matkaviestimen salauksen suorittavalle välineelle välitetään edullisesti tilaajan tunnistussovellukselle, kuten SIM-sovellukselle, talletettu toinen salausavain. Näin voidaan heti yhteyden siirryttyä toisen matkaviestinverkon tukiasemajärjestelmään siirtyä käyttämään sekä matkaviestimessä että toisen matkaviestinverkon salauksen suorittavassa verkkoelementissä kyseisen verkon mukaista salausta. Tällöin saavutetaan se etu, että handoverin jälkeen liikennettä ei siirry salaamattomana ilmarajapinnan yli ensimmäisiä signalointiviestejä lukuunottamatta, kuten GSM-järjestelmän sisäisessä handover-tilanteessa.

Keksinnön mukaisen ratkaisun mukaisesti matkaviestinverkko ja matkaviestin voivat käyttää useampaa erilaista, vaihtoehtoista, salausta tai autentikaatiota käyttämällä eri algoritmeja tai avaimia. Näin voidaan matkaviestinverkon ja matkaviestimen tukiessa useampaa kuin yhtä salaus- tai autentikaatiomenetelmää esimerkiksi vaihtaa käytettävää salausavainta tarpeen mukaan.

Keksinnön erään edullisen suoritusmuodon mukaan ensimmäinen matkaviestinverkko tutkii esimerkiksi IMSI- ja/tai classmark-tunnisteen avulla,

tukeeko matkaviestin toista matkaviestinverkkoa. Tällöin toisen matkaviestinjärjestelmän mukaisen salausavaimen laskeminen suoritetaan edullisesti ainoastaan, jos matkaviestin tukee toista matkaviestinverkkoa. Edelleen voidaan keksinnön erään edullisen suoritusmuodon mukaan suorittaa toisen salausavaimen laskeminen samanaikaisesti, kun suoritetaan ensimmäisen matkaviestinjärjestelmän mukainen autentikaatio. Tällöin voidaan edullisesti yhdellä viestillä pyytää autentikaatiokeskukselta ja edelleen matkaviestimeltä kahden eri järjestelmän mukaisen salausavaimen ja mahdollisesti autentikaatiovasteen laskemista.

Toisaalta keksinnön erään edullisen suoritusmuodon mukaan voidaan eritellä pyyntö nimenomaan toisen matkaviestinjärjestelmän mukaisen toisen salausavaimen laskemiseksi. Tämä voi olla tarpeen esimerkiksi, kun havaitaan, että on tarpeen suorittaa handover toiseen matkaviestinverkkoon. Tällöin voidaan pyytää ainoastaan toisen matkaviestinverkon mukaisen salausavaimen laskemista edullisesti autentikaation yhteydessä. Keksinnön mukaan toinen salausavain voidaan laskea ainoastaan tarvittaessa, eli esimerkiksi, kun tehdään päätös handoverista toiseen matkaviestinverkkoon.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää esimerkinomaisesti UMTS-järjestelmää, johon on myös kytketty GSM-tukiasemajärjestelmä;

Kuvio 2 esittää vuokaavion avulla keksinnön mukaista menetelmää yksinkertaistettuna;

Kuvio 3 esittää erästä keksinnön mukaisen autentikaation toteutusta signalointikaavion avulla;

Kuvio 4 esittää esimerkinomaisesti handover-toimintoa UMTS-järjestelmästä GSM-järjestelmään signalointikaavion avulla.

Keksinnön yksityiskohtainen selostus

Keksintöä voidaan soveltaa periaatteessa mihin tahansa matkaviestinjärjestelmään. Erityisen hyvin se soveltuu UMTS-järjestelmään, joka tulee monelta osin perustumaan GSM-järjestelmään. Seuraavassa keksintöä tullaan selostamaan käyttäen esimerkkiä, jossa UMTS-verkossa suoritetaan GSM-autentikaatiotoimintoja, erityisesti salausavaimen laskeminen, ennen handover-toimintoa UMTS-verkosta GSM-verkkoon (Kuviot 1 ja 3) ja handover-

toimintoa, jossa hyödynnetään keksinnön mukaan ennalta laskettua salausavainta (Kuvio 4). Kuviossa 2 kuvataan pelkistetysti keksinnön mukaista menetelmää riippumatta käytettävästä matkaviestinjärjestelmästä.

Kuviossa 1 on esitetty esimerkinomaisesti eräs UMTS-järjestelmän mukainen matkaviestinverkko, jonka ydinverkko CN (Core Network) voi ohjata myös GSM-tukiasemajärjestelmää. UMTS-matkaviestin MS (Mobile Station) käsittää puhelinlaitteen ME (Mobile Equipment) ja UICC-älykortin. UMTS-tukiasemajärjestelmä RAN (Radio Access Network) käsittää yhden tai useamman tukiaseman BS (Base Station), joiden käytettävissä olevia radiotaajuuksia ja kanavia tukiasemaohjain RNC (Radio Network Controller) kontrolloi.

Piirikytkentäisille palveluille tukiasemaohjaimet RNC on kytketty matkaviestinkeskukseen MSC, joka huolehtii piirikytkentäisten palveluiden yhteydenmuodostuksesta ja reitittämisestä oikeisiin osoitteisiin. Tässä käytetään apuna kahta tietokantaa, jotka käsittävät tietoa matkaviestintilaajista: kotirekisteriä HLR ja vierailijarekisteriä VLR. Vastaavasti pakettikytkentäisille palveluille on käytössä SGSN (Serving GPRS Support Node), joka käyttää apunaan kotirekisteriä HLR. Sekä MSC että SGSN ovat yhteydessä autentikaatiokeskukseen AuC tyypillisesti kotirekisterin HLR kautta.

Matkaviestinkeskus MSC on yhteydessä yhdyskäytävän IWF (Interworking Function) kautta muihin tietoliikenneverkkoihin, kuten esimerkiksi PSTN-verkkoon (Public Switched Telephone Network) tai ISDN-verkkoon (Integrated Services Digital Network). GPRS-yhteyskäytävä GGSN (GPRS Gateway Support Node) on yhteydessä pakettipohjaisiin tietoliikenneverkkoihin PDN (Packet Data Network).

Ydinverkkoon CN on kytketty myös GSM-järjestelmän mukainen tukiasemajärjestelmä BSS, joka käsittää ainakin yhden tukiaseman BTS (Base Transceiver Station) ja tukiasemaohjaimen BSC (Base Station Controller).

3GPP:n UMTS-dokumenteissa määritelty kotiverkko HE (Home Environment) tekee tilaajan kanssa sopimuksen palveluiden tarjonnasta ja antaa USIM-sovelluksen. Tällöin kotirekisteri HLR sijaitsee kotiverkossa HE. Palveleva verkko SN (Serving Network) tarkoittaa verkkoa, jonka alueella matkaviestin kulloinkin on. Roaming-tilanteissa tai tilanteissa, joissa palveluntarjonta ja verkon operointi on erotettu toisistaan, kotiverkko HE ja palveleva verkko SN ovat eri tahoja. Kuviossa 1 ei ole eroteltu kotiverkkoa HE ja palvelevaa verkkoa SN.

Myöhemmin kuvattavissa toiminnoissa vierailijarekisteri VLR voi sijaita palvelevassa verkossa SN ja autentikaatiokeskus AuC voi sijaita eri operaattorin kotiverkossa HE tai ne voivat kuulua myös saman operaattorin alaiseen verkkoon. Tämän hakemuksen yhteydessä kuvion 1 ydinverkon CN verkkoelementit on nimetty kuten GSM-järjestelmässä, olennaista on, että verkkoelementit kykenevät suorittamaan UMTS-järjestelmän mukaiset toiminnot.

UMTS-järjestelmän turvallisuusarkkitehtuuri tulee olemaan samankaltainen kuin GSM-järjestelmässä. Tällöin aiemmin kuvattu GSM:n mukainen menettely tullaan toteuttamaan myös UMTS:ssä, seuraavassa on käsitelty odotettavissa olevia eroavaisuuksia. Taulukossa 1 esitetään GSM-parametrejä vastaavat UMTS-parametrit, joita on käsitelty 3GPP:n dokumentissa TR S3.03 versio 0.1.2 "3G Security: Security Architecture".

Taulukko 1.

SELITYS	GSM	UMTS
satunnaislukuparametri	RAND	RANDu
verrattava autentikaation tarkistusparametri (autentikaatiovaste)	SRES	XRES
salausavain	Kc	CK
integriteettiavain	-	IK
varmistustunniste	-	AUTN

UMTS-järjestelmän mukaisessa autentikaatiossa autentikaatiokeskus AuC muodostaa taulukon 1 mukaiset viisi parametriä ja välittää ne vierailijarekisteriin VLR. GSM-järjestelmässä muodostetaan kolme parametriä eli tripletti. Satunnaislukuparametri RANDu (Random Number) vastaa GSM:n RAND-parametriä, mutta voi olla eri pituinen. Odotettu tarkastusparametri XRES (Expected Response) ja erityisesti salausavain CK (Cipher Key) voivat myös olla eri pituisia GSM-parametreihin SRES ja Kc verrattuna. Varmistustunnistetta AUTN (Authentication Token) ei ole GSM:ssä, se voidaan lähettää USIM-sovellukselle samassa viestissä kuin RANDu-parametri. AUTN-tunnisteen avulla USIM-sovellus voi tarkastaa onko palveleva verkko oikeutettu tarjoamaan UMTS-palveluja. Erona GSM-järjestelmään, USIM muodostaa XRES-parametrin ja laskee salausavaimen CK vain, jos AUTN-parametri

on hyväksyttävä. Kuten GSM-järjestelmässä, USIM välittää laskemansa XRES-parametrin verkkoon vierailijarekisteriin VLR, joka vertaa sitä autentikaatiokeskukselta saamaansa autentikaation tarkastusparametriin. Autentikaatio on onnistunut, jos verkossa laskettu XRES ja USIM-sovelluksessa laskettu XRES-parametri vastaavat toisiaan.

Integriteettiavainta IK (Integrity Key) ei ole GSM-järjestelmässä, UMTS:ssä sitä tullaan käyttämään tiettyjen signalointiviestien, kuten esimerkiksi matkaviestimen ominaisuustietojen suojaamiseen. IK lasketaan sekä USIM-sovelluksessa että UMTS-verkossa. Koska UMTS-standardointityö on kesken, kyseisten taulukossa 1 esitettyjen parametrien muodostamiseen tarvittavia algoritmeja ei ole vielä määritetty tarkasti. Ne todennäköisesti tulevat eroamaan GSM:n algoritmeista A3, A5 ja A8. GSM:n salaista avainta Ki vastaava avain UMTS:ssä on K, jota käytetään autentikaatioparametrien laskennassa sekä USIM-sovelluksessa että autentikaatiokeskuksessa.

GSM- tai UMTS-verkko voi periaatteessa pyytää autentikaatiota matkaviestimeltä milloin tahansa. Autentikaatio voidaan suorittaa esimerkiksi sijainninpäivityksen (location update) yhteydessä tai vastattaessa paging-kutsuun (paging response) matkaviestimeen tulevan puhelun tapauksessa. Keksintöä voidaan soveltaa missä tahansa vaiheessa tapahtuvaan autentikaatioon.

Keksinnön mukaisessa esimerkissä matkaviestin MS kykenee muodostamaan yhteyden sekä GSM- että UMTS-verkkoihin, eli se on ns. dual-mode-matkaviestin. MS käsittää tällöin sekä GSM-järjestelmän että UMTS-järjestelmän mukaiset toiminnot ja edelleen SIM-sovelluksen toiminnot ja USIM-sovelluksen toiminnot. SIM/USIM-toiminnot edullisesti sijaitsevat älykortilla UICC ja ne voivat edullisesti olla samalta operaattorilta eli kotiverkolta HE yhtenä sovelluksena. Oletuksena on, että tilaajatunnus, edullisesti IMSI, on sama sekä GSM- että UMTS-järjestelmälle. Tällöin IMSI-tunnus identifioi sekä SIM-sovelluksen että USIM-sovelluksen. UMTS-verkko voi edullisesti myös havaita IMSI-tunnuksen perusteella, onko kyseessä sekä GSM- että UMTS-palveluihin oikeutettu tilaaja. Vaikka IMSI-tunnus onkin sama, autentikaatio (käsittäen salausavainten laskemisen) voidaan kuitenkin keksinnön mukaisessa ratkaisussa suorittaa sekä SIM-sovellukselle että USIM-sovellukselle erikseen.

Seuraavassa kuvataan keksinnön mukaista menetelmää pelkistetysti kuvion 2 avulla, jolloin ei olla sitouduttu mihinkään tiettyyn matkaviestin-

järjestelmään. Kuviossa 2 keksinnön tärkeimpiä vaiheita on yksinkertaistettu ja kaikkia suoritusmuotoja ei ole kuvattu. Myöhemmin kuvioiden 3 ja 4 avulla kuvataan tarkemmin eri vaiheita ja suoritusmuotoja UMTS- ja GSM-järjestelmiin sovellettuna.

Matkaviestimen toimiessa ensimmäisessä matkaviestinverkossa, ilmarajapinnan yli siirtyvä liikenne pääsääntöisesti salataan käyttäen ensimmäistä salausavainta. Keksinnön mukaan ensimmäisessä matkaviestinverkossa lasketaan toisen matkaviestinverkon mukainen toinen salausavain (20). Tämä voi tapahtua esimerkiksi ensimmäisen matkaviestinverkon havaittua tarve aktiivisen yhteyden siirrolle toiseen matkaviestinverkkoon tai ensimmäisen matkaviestinverkon mukaisen autentikaation yhteydessä.

Laskettuaan toisen salausavaimen, ensimmäinen matkaviestinverkko välittää salausavaimen laskemiseen tarvittavat tiedot matkaviestimelle (21). Matkaviestin havaitsee, että on kyse toisen matkaviestinverkon mukaisen toisen salausavaimen laskemisesta ja suorittaa toisen salausavaimen laskemisen (22). Tämän jälkeen toinen salausavain on käytettävissä sekä ensimmäisessä matkaviestinverkossa että matkaviestimessä. Jos matkaviestimen käytössä oleva yhteys siirretään toiseen matkaviestinverkkoon, käytetään yhteyden siirron jälkeen sekä matkaviestimessä että toisessa matkaviestinverkossa toista salausavainta (23). Tällöin ensimmäinen matkaviestinverkko on edullisesti välittänyt toisen avaimen toisen matkaviestinverkon salauksen suorittavalle verkkoelementille ennen yhteydensiirtoa. Näin matkaviestimen ja toisen matkaviestinverkon välinen liikenne voidaan salata heti yhteydensiirron jälkeen.

Seuraavassa selostetaan keksinnön mukaista ratkaisua tarkemmin sovellettuna UMTS- ja GSM-verkkoihin kuvion 3 avulla. Kuviossa 3 on esitetty esimerkinomainen signalointikuvio keksinnön mukaisesta autentikaatioprosessista eli salausavaimen muodostamisesta, autentikaatioparametrien muodostamisesta ja tarkastamisesta vain keksinnön kannalta olennaiset vaiheet mukaan ottaen. Matkaviestimen ollessa UMTS-verkon alueella, oletetaan myös, että matkaviestimen ja matkaviestinverkon välinen liikenne salataan UMTS-salausavainta käyttäen.

Kuviossa 3 matkaviestin MS välittää esimerkiksi location update request-viestin pyytääkseen sijainninpäivitystä (identity, nuoli 30). Olennaista on, että viesti (identity, nuoli 30) käsittää UMTS-tilaajatunnisteen, joko TMSI- tai IMSI-tunnisteen vastaavaa tarkoitusta varten kuin GSM-järjestelmässä eli ti-

laajan identifioimiseksi. Joissakin UMTS-spesifikaatioissa TMSI-tunnusta vastaa TMUI (Temporary Mobile User Identity) ja IMSI-tunnusta IMUI (International Mobile User Identity).

UMTS-verkko voi myös lähettää pyynnön matkaviestimelle tilaajatunnisteen lähettämiseksi, johon matkaviestin vastaa lähettämällä pyydetyn tilaajatunnisteen (identity, nuoli 30).

On edelleen mahdollista, että UMTS-järjestelmässä salataan IMSI-tunnus radiotien yli väärinkäytösten estämiseksi. Jos IMSI-tunnus on salattu, vierailijarekisterin VLR on välitettävä salattu IMSI-tunnus kotirekisteriin HLR, joka välittää salaamattoman IMSI-tunnuksen takaisin vierailijarekisteriin (ei kuvattu).

Vierailijarekisteri VLR välittää pyynnön autentikaatiosta ja IMSI-tunnuksen kotirekisteriin HLR ja edelleen autentikaatiokeskukseen AuC (send authentication info, nuoli 31). Verkossa VLR ja HLR kommunikoivat käyttäen MAP-signalointiprotokollaa. UMTS-järjestelmässä voidaan käyttää eri MAP-versiota kuin GSM:ssä, koska edellä kuvatut UMTS:n autentikaatiotoiminnot eivät toimi ilman muutoksia MAP-protokollassa. Näinollen kotiverkko HE ja edelleen kotirekisterin yhdessä oleva autentikaatiokeskus AuC voi päätellä esimerkiksi MAP-versiosta, että pyyntö (send authentication info, nuoli 31) on tullut UMTS-järjestelmän osaavasta verkosta.

Kotiverkko HE, edullisesti kotirekisteri HLR, voi havaita IMSI-tunnuksen perusteella, että tilaajalla on oikeus sekä GSM- että UMTS-verkon käyttöön. Keksinnön erään edullisen suoritusmuodon mukaan autentikaatiokeskus AuC laskee sekä UMTS:n autentikaatioparametrit että GSM:n autentikaatioparametrit (tripletin) olennaisesti samanaikaisesti ja välittää ne vierailijarekisteriin VLR. Jos palveleva verkko SN ei ole UMTS-järjestelmän mukainen (esimerkiksi GSM-järjestelmän mukainen MAP-versio) tai IMSI-tunnuksen perusteella ainoastaan SIM-sovellus on käytettävissä, autentikaatiokeskus AuC laskee edullisesti ainoastaan GSM-autentikaatioparametrit. Edelleen GSM-parametrien laskemisen ehtona voi olla matkaviestimen MS ominaisuudet, eli tukeeko matkaviestin GSM-järjestelmää. Tällöin vastaavasti matkaviestimen tukiessa ainoastaan UMTS-järjestelmää tai IMSI-tunnuksen perusteella ainoastaan USIM-sovelluksen ollessa käytettävissä, AuC voi laskea ainoastaan UMTS:n autentikaatioparametrit.

Vaihtoehtoisesti on mahdollista, että vierailijarekisteri VLR pyytää (send authentication info, nuoli 31)-viestin yhteydessä haluamansa järjestel-

män tai järjestelmien mukaista autentikaatiotietoa. Tämä voidaan toteuttaa esimerkiksi lisäämällä autentikaatiotietojen pyyntöön (send authentication info, nuoli 31) bitit, jotka kertovat pyydetyn järjestelmän autentikaatiotyypin.

Turhan laskentatehon kulutuksen välttämiseksi, UMTS-verkossa suoritetaan GSM-autentikaatio edullisesti ainoastaan, jos matkaviestin käsittää SIM-sovelluksen ja GSM-toiminnallisuuden (dual-mode-matkaviestin). UMTS-verkko voi esimerkiksi classmark-tunnuksesta erottaa, tukeeko matkaviestin GSM-järjestelmää. Tällöin vierailijarekisteri VLR voi classmark-tunnuksen ja/tai IMSI-tunnuksen ilmaistua matkaviestimen tukevan GSM-järjestelmää pyytää autentikaatiokeskukselta AuC sekä GSM- että UMTS-järjestelmän mukaista autentikaatiota (send authentication info, nuoli 31)-viestin yhteydessä.

Autentikaatiokeskus AuC välittää laskemansa autentikaatiotiedot vierailijarekisteriin VLR (authentication info, nuoli 32), johon ne talletetaan. Koska autentikaatiokeskus on laskenut GSM-autentikaatioparametrit, GSM-verkon mukainen salausavain Kc on myöhempää tarvetta varten käytettävissä palvelevassa verkossa SN. Keksinnön mukaista ideaa voidaan tämän vaiheen jälkeen soveltaa ainakin kahdella erilaiselle tavalla, implisiittisellä tai eksplisiittisellä GSM-autentikaatiolla, joita kuvataan seuraavaksi.

Seuraavassa käsitellään keksinnön erään edullisen suoritusmuodon mukaista implisiittistä GSM-autentikaatiota. Tässä tapauksessa autentikaatiokeskukselta AuC vastaanotettu UMTS satunnaislukuparametri RANDu on samanpituinen GSM satunnaislukuparametrin RAND kanssa (edullisesti 128 bittiä). VLR välittää matkaviestimelle autentikaatiopyynnön (authentication request, nuoli 33), joka käsittää GSM-järjestelmän RAND-parametrin pituisen satunnaislukuparametrin RANDu. Koska kyseessä on UMTS-järjestelmän mukainen autentikaatio, matkaviestimen USIM-sovellukselle välitetään edullisesti myös varmistustunniste AUTN.

Matkaviestin MS välittää keksinnön erään edullisen suoritusmuodon mukaisesti satunnaislukuparametrin RANDu sekä SIM- että USIM-sovelluksille, vaikka autentikaatiopyyntö (authentication request, nuoli 33) olisikin UMTS-järjestelmän mukainen. Matkaviestimessä voi olla esimerkiksi välineet satunnaislukuparametrin tarkistamiseksi, jolloin satunnaislukuparametrin ollessa GSM-järjestelmän mukainen, välitetään se myös SIM-sovellukselle. Tällöin keksinnön erään edullisen suoritusmuodon mukaisesti SIM-sovellus laskee salausavaimen Kc käyttäen salaista avainta Ki ja RANDu-parametria A8-algoritmin avulla. SIM-sovelluksen ei kuitenkaan tarvitse muo-

dostaa autentikaation tarkistusparametria SRES. SIM-sovellus tallettaa Kc:n myöhempää käyttöä varten edullisesti älykortin UICC muistiin.

USIM-sovellus vastaanottaa RANDu-parametrin, ja jos varmistustunniste AUTN on hyväksyttävä, suorittaa autentikaation tarkistusparametrin XRES laskemisen. Tällöin salaista avainta K ja RANDu-parametria UMTS:n autentikaatioalgoritmin avulla USIM muodostaa XRES-parametrin. Samanaikaisesti voidaan laskea UMTS:n salausavain CK salaisen avaimen K ja salausavaimen laskemisalgoritmin avulla. Autentikaation tarkistusparametri XRES välitetään USIM-sovellukselta vierailijarekisteriin VLR (authentication response, nuoli 34), joka vertaa sitä autentikaatiokeskuksesta AuC saamaansa tarkistusparametriin. Jos ne vastaavat toisiaan, UMTS:n mukainen autentikaatio on onnistunut.

Keksinnön erään edullisen suoritusmuodon mukaan implisiittisessä GSM-autentikoinnissa oletetaan myös GSM-autentikaatio suoritetuksi, kun UMTS autentikaatio on onnistunut. Edelleen GSM-järjestelmän mukainen salausavain on olemassa sekä UMTS-verkossa että USIM-sovelluksessa mahdollista handoveria UMTS-verkosta GSM-verkkoon varten. Kun autentikaatio on suoritettu, UMTS-verkko voi välittää hyväksynnän eli kuittauksen autentikaatiosta matkaviestimelle MS (acknowledgement, nuoli 35). Tällöin voidaan jatkaa kulloinkin tarpeen olevia toimenpiteitä tunnetun tekniikan mukaisesti, esimerkiksi UMTS-verkko voi antaa matkaviestimelle MS käskyn salauksen aloittamisesta.

Koska implisiittisessä GSM autentikaatiossa on tarpeen suorittaa ainoastaan salausavaimen Kc laskeminen, autentikaatiokeskuksen AuC ei ole välttämätöntä laskea ja välittää vierailijarekisteriin VLR kaikkia autentikaatioparametrejä. Ainoastaan salausavain Kc on laskettava ja välitettävä vierailijarekisteriin käyttäen edullisesti samaa satunnaislukuparametriä kuin UMTS:n salausavaimen CK laskemisessa.

Keksinnön erään edullisen suoritusmuodon mukaan voidaan suorittaa myös ns. eksplisiittinen GSM-autentikaatio. Tällöin RANDu-parametri voi olla erityinen GSM:n RAND-parametriin verrattuna. Tällöin UMTS-verkko välittää edullisesti autentikaatiopyynnössä (authentication request, nuoli 33) tiedon siitä, halutaanko GSM-autentikaatio, UMTS-autentikaatio vai mahdollisesti molemmat.

Autentikaatiopyyntö (authentication request, nuoli 33) esimerkiksi käsittää GSM-bitin ja UMTS-bitin. Kun GSM-bitti on arvoltaan 1, matkaviestin havaitsee, että pyydetään GSM-autentikaatiota. Vastaavasti, jos UMTS-bitti on

1, suoritetaan UMTS-järjestelmän mukainen autentikaatio. Jos molemmat bitit ovat 1, voidaan suorittaa molempien järjestelmien mukainen autentikaatio. MS voi havaita halutun autentikaation myös satunnaislukuparametrin RAND tai RANDu pituudesta. Edelleen matkaviestin MS voi erottaa, että halutaan UMTS-autentikaatiota, jos autentikaatiopyyntö (authentication request, nuoli 33) käsittää varmistustunnisteen AUTN.

Jos palveleva verkko HE on pyytänyt GSM-autentikaatiota, välitetään RAND-satunnaislukuparametri SIM-sovellukselle ja suoritetaan GSM-järjestelmän mukainen autentikaatiovasteen SRES ja salausavaimen Kc laskeminen. Autentikaatiovaste SRES välitetään vierailijarekisterille VLR tarkastettavaksi (authentication response, nuoli 34) ja salausavain Kc talletetaan mahdollista myöhempää käyttöä varten SIM-sovellukselle.

Jos palveleva verkko HE on pyytänyt UMTS-autentikaatiota, välitetään RANDu-satunnaislukuparametri USIM-sovellukselle ja suoritetaan UMTS-järjestelmän mukainen autentikaatio jo aiemmin kuvatun tavan mukaisesti. Jos UMTS-autentikaatio onnistuu, sen perusteella ei kuitenkaan oleteta GSM-autentikaatiosta mitään, vaan GSM-autentikaatio on suoritettava erikseen palvelevan verkon SN niin halutessa.

Jos palveleva verkko HE pyytää sekä GSM- että UMTS-järjestelmän mukaista autentikaatiota, se edullisesti välittää sekä RANDu- että RAND-parametrit autentikaatiopyynnössä (authentication request, nuoli 33). Matkaviestimen havaittua esimerkiksi kahdesta eri satunnaislukuparametristä, että pyydetään sekä UMTS- että GSM-autentikaatiota, se välittää RAND-parametrin SIM-sovellukselle ja RANDu-parametrin USIM-sovellukselle. SIM ja USIM suorittavat autentikaatiovasteiden SRES ja XRES sekä salausavainten Kc ja CK laskemisen. Matkaviestin MS välittää SIM-sovelluksen välittämän SRES-parametrin ja USIM-sovelluksen välittämän XRES-parametrin vierailijarekisterille VLR (authentication response, nuoli 34) mahdollisesti eri viesteissä. Vierailijarekisteri VLR vertaa matkaviestimeltä MS saatuja autentikaatiovasteita autentikaatiokeskukselta AuC saatuihin, ja jos ne täsmäävät, autentikaatiot ovat onnistuneet.

Edellä kuvattua eksplisiittistä menetelmää voidaan yleisesti soveltaa matkaviestinjärjestelmään, joka tukee useita autentikaatiomenetelmiä. Esimerkiksi UMTS-järjestelmään voidaan kehittää myöhemmin uusi, vaihtoehtoinen autentikaatio ja/tai salausmenetelmä. Autentikaation ja salausavaimen laskemisen suorittava verkkoelementti (esimerkiksi AuC) ja matkaviestimessä vastaavat

toiminnot suorittava väline (esimerkiksi USIM) käsittävät samat algoritmit. Jos myös palveleva matkaviestinverkko ja erityisesti vierailijarekisterin VLR toimintoja suorittava verkkoelementti osaavat käyttää vaihtoehtoisen autentikaatiomenetelmän mukaisia parametrejä, voidaan toimia keksinnön idean mukaisesti. Tällöin palveleva matkaviestinverkko voi välittää autentikaatiokeskukselle AuC tunnisteen esimerkiksi käytettävästä autentikaatioalgoritmista tai algoritmeista.

Toisaalta on myös mahdollista, että AuC on tietoinen matkaviestimen ja edelleen palvelevan matkaviestinverkon ominaisuuksista. Tällöin se voi välittää ominaisuuksien perusteella myös vaihtoehtoisen tavan mukaiset parametrit palvelevaan matkaviestinverkkoon, esimerkiksi vierailijarekisteriin VLR. Edelleen palveleva matkaviestinverkko voi edullisesti välittää matkaviestimelle tiedon käytettävästä autentikaatiomenetelmästä esimerkiksi autentikaatiopyynnön yhteydessä. Näin voidaan esimerkiksi joustavasti vaihtaa käytettävää salausmenetelmää laskemalla uuden autentikaation mukainen salausavain sekä autentikaatiokeskuksessa että tilaajasovelluksessa. Käytettävä salausmenetelmä voidaan tarvittaessa vaihtaa välittämällä uusi salausavain salauksen hoitaville välineille sekä matkaviestinverkossa että matkaviestimessä. Edullisesti onnistuneesta salausmenetelmän vaihdosta välitetään tieto myös autentikaatiokeskukseen AuC.

Edellä kuvatulla keksinnön mukaisella implisiittisen tai eksplisiittisen tavan mukaisella GSM-autentikaatiolla saavutetaan se huomattava etu, että GSM-järjestelmän mukainen salausavain Kc on valmiina mahdollista handoveria UMTS-järjestelmästä GSM-järjestelmään varten. Salausavain Kc on talletettuna sekä UMTS-verkossa, edullisesti vierailijarekisterissä VLR, että matkaviestimessä, edullisesti SIM-sovelluksessa.

GSM-järjestelmän mukaisen salausavaimen Kc laskeminen voidaan suorittaa palvelevan verkon SN niin halutessa. Se voidaan suorittaa esimerkiksi aina UMTS-autentikaation yhteydessä.

Salausavaimen Kc laskeminen voidaan keksinnön erään edullisen suoritusmuodon mukaan tehdä myös havaittaessa ympäröivien radiosolujen mittaustuloksista, että on tarve tehdä handover GSM-järjestelmän mukaiseen tukiasemajärjestelmään BSS. Edelleen salausavain Kc voidaan laskea handoveria toteutettaessa, jolloin kuitenkin voi aiheutua viivettä handoverin suorittamiseen.

GSM-järjestelmän mukainen salausavain Kc voidaan määrittää myös erottamalla se UMTS:n salausavaimesta CK esimerkiksi siirrettäessä

yhteyttä GSM-tukiasemaan. Oletettavasti CK tulee olemaan pidempi kuin Kc. Tällöin matkaviestin MS ja UMTS-verkko, edullisesti VLR, lyhentävät CK-avaimesta Kc-avaimen pituisen ja edullisesti tallettavat muistiin myöhempää käyttöä varten. Näin GSM-järjestelmän mukainen Kc-avain on käytettävissä mahdollista handover-tilannetta varten. Tällöin ei tarvitse suorittaa GSM-parametrien laskemista autentikaatiokeskuksessa eikä SIM-sovelluksessa.

Seuraavassa on kuvattu kuvion 4 avulla handover-prosessia piirikytkentäisessä yhteydessä esimerkinomaisesti vain keksinnön kannalta olennaiset osat huomioon ottaen. Matkaviestin MS suorittaa mittauksia lähialueen tukiasemista, mitaten myös GSM-järjestelmän tukiasemia UMTS-verkon edullisesti niin pyydettyä. Matkaviestin MS välittää mittaustiedot sitä palvelevalle tukiaseman ohjaimelle RNC (measurement, nuoli 40).

RNC tekee päätöksen inter-system handoverista perustuen esimerkiksi handover-kynnyksen ylityttyä signaalinvoimakkuuden osalta. RNC välittää ilmoituksen handoverin tarpeellisuudesta palvelevan UMTS-verkon (SN) matkaviestinkeskukselle AMSC (Anchor MSC) (handover required, nuoli 41). AMSC on handoverissa ns. lähdematkaviestinkeskus. AMSC käsittää edullisesti sovitustoimintoja (Interworking Function, IWF), jolloin voidaan muodostaa GSM-järjestelmän mukainen handover-pyyntö. Jos salausavainta Kc ei ole etukäteen laskettu, AMSC voi pyytää sen laskemista esimerkiksi handover-pyynnön (handover required, nuoli 41) saatuaan. Ennen handover-pyynnön välittämistä GSM-verkkoon, on suoritettu salausavaimen Kc laskeminen esimerkiksi aiemmin kuvatun eksplisiittisen tavan mukaisesti.

AMSC hakee ennalta lasketun salausavaimen Kc edullisesti vierailijarekisteristä VLR. AMSC välittää salausavaimen Kc muun GSM-järjestelmän mukaisen handoverissa tarvittavan tiedon, kuten matkaviestimen classmark-tiedon, ohella handover-pyynnössä GSM-järjestelmän mukaiseen kohdematkaviestinkeskukseen RMSC (Relay MSC) (prepare ho request, nuoli 42). On mahdollista, että UMTS-tukiasemajärjestelmä ja handoverin kohteena oleva GSM-tukiasemajärjestelmä ovat saman ydinverkon yhteydessä kuten kuviossa 1 on havainnollistettu. Tällöin sekä GSM- että UMTS-tukiasemajärjestelmää voi ohjata sama matkaviestinkeskus MSC, joka välittää pyynnön handoverista GSM-tukiasemajärjestelmään GSM-järjestelmän mukaisesti.

RMSC välittää pyynnön handoverista, joka käsittää myös salausavaimen Kc, tukiasemaohjaimelle BSC (handover request, nuoli 43). BSC varaa tarvittavat resurssit handover-pyynnön mukaisesti ja välittää vastauksen

RMSC:lle (ho request ack, nuoli 44). RMSC välittää vastauksen handover-pyynnölle AMSC:lle (prepare ho response, nuoli 45). AMSC välittää UMTS-järjestelmän mukaisen komennon handoverin suorittamiseksi tukiasemaohjaimelle RNC (handover command, nuoli 46).

RNC välittää matkaviestimelle MS komennon UMTS- ja GSM-järjestelmien välisestä handoverista (inter-system ho command, nuoli 47). Tämä viesti käsittää kaiken tarvittavan tiedon mm. radiokanavasta matkaviestimelle, että se voi suorittaa GSM-järjestelmän mukaisen handoverin. Matkaviestin MS tunnistaa, että kyseessä on handover GSM-järjestelmään, jolloin se aktivoi GSM-toiminnot. Edelleen matkaviestin edullisesti havaitsee, että tarvitaan GSM-järjestelmän mukainen salausavain, jolloin pyydetään SIM-sovellukselta GSM-järjestelmän mukaista salausavainta Kc. SIM-sovellus välittää salausavaimen Kc matkaviestimen GSM-järjetelmän mukaisen salauksen suorittavalle välineelle.

Matkaviestin MS välittää sille allokoidulla GSM-kanavalla handover access-viestin aivan kuten tyypillisessä GSM-järjestelmässä (handover access, nuoli 48). Matkaviestin MS välittää tyypillisesti yhden tai useamman GSM-spesifikaatioissa määritetyn [HANDOVER ACCESS]-viestin, jotka eivät ole salattuja. Tämän jälkeen yhteys siirretään GSM tukiasemajärjestelmän palveltavaksi sinänsä jo tunnetun GSM-tekniikan mukaisesti, jota ei ole tarpeen tässä yhteydessä tarkemmin kuvata. Siirrettävä liikenne voidaan keksinnön mukaisesti salata käyttäen etukäteen laskettua salausavainta Kc ja salausalgoritmiä A5 edullisesti heti (handover access, nuoli 48)-viestin jälkeen. GSM-verkko voi myös mahdollisesti suorittaa autentikaation, vaikka liikenne voidaankin jo salata.

Keksinnön mukaisesta ratkaisusta saadaan se huomattava etu, että matkaviestimen ja matkaviestinverkon välinen liikenne voidaan salata heti handoverin jälkeen GSM-järjestelmän mukaisen salausavaimen Kc avulla. Jos salausavainta Kc ei olisi käytettävissä matkaviestimessä ja GSM-tukiasemassa salausta varten, jouduttaisiin tekemään autentikaatio ja salausavaimen laskeminen handoverin jälkeen GSM-verkossa. Tällöin osa siirrettävästä tiedosta jäisi salaamatta ja aikaa kuluisi.

Keksinnön toteuttamiseksi tarvitaan muutoksia lähinnä matkaviestinkeskuksen MSC/VLR, vierailijarekisterin VLR ja matkaviestimen MS toimintoihin tunnetun tekniikan, kuten GSM-järjestelmän, toteutukseen verrattuna.

Keksinnön mukaisen ratkaisun vaatimat toiminnot voidaan toteuttaa ohjelmallisesti.

Edellä kuvattu autentikaatio, salausavaimen laskeminen ja handoverin toteuttaminen kuvaavat esimerkinomaisesti keksinnön soveltamista UMTS- ja GSM-järjestelmiin. Keksintöä voidaan hyvin soveltaa myös muihin matkaviestinjärjestelmiin, kuten langattomiin lähiverkkojärjestelmiin, eri tavoin soveltaen.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

Patenttivaatimukset

1. Menetelmä tietosuojauksen järjestämiseksi tietoliikennejärjestelmässä, joka käsittää ensimmäisen matkaviestinverkon, jossa käytetään ensimmäistä salausavainta matkaviestimen ja matkaviestinverkon välisen liikenteen salaamiseen, toisen matkaviestinverkon, jossa käytetään toista salausavainta matkaviestimen ja matkaviestinverkon välisen liikenteen salaamiseen ja mainittuja matkaviestinverkkoja tukevan matkaviestimen, t u n n e t t u siitä, että

suoritetaan mainitun toisen salausavaimen laskeminen ensimmäisessä matkaviestinverkossa, kun matkaviestin toimii ensimmäisessä matkaviestinverkossa,

välitetään toisen salausavaimen laskemiseen tarvittavat tiedot ensimmäisestä matkaviestinverkosta mainittuun matkaviestimeen, kun matkaviestin toimii ensimmäisessä matkaviestinverkossa ja

lasketaan toinen salausavain matkaviestimessä.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

käytetään mainittua toista salausavainta matkaviestimen ja toisen matkaviestinverkon välisen liikenteen salaukseen, jos matkaviestin siirtyy aktiivisen yhteyden aikana ensimmäisestä matkaviestiverkosta toiseen matkaviestinverkkoon.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että

välitetään mainittu toinen salausavain mainitusta ensimmäisestä matkaviestinverkosta mainittuun toiseen matkaviestinverkkoon,

välitetään mainitun matkaviestimen salauksen suorittavalle välineelle matkaviestimessä laskettu mainittu toinen salausavain vasteena sille, että ensimmäinen matkaviestinverkko välittää pyynnön matkaviestimelle yhteydensiirrosta toiseen matkaviestinverkkoon ja

käytetään mainittua toista salausavainta liikenteen salaamisessa yhteydensiirron jälkeen mainitussa matkaviestimessä ja mainitussa toisessa matkaviestinverkossa.

4. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

tarkastetaan ensimmäisessä matkaviestinverkossa, tukeeko mainittu matkaviestin mainittua toista matkaviestinverkkoa,

suoritetaan mainitun toisen salausavaimen laskeminen mainitussa ensimmäisessä matkaviestinverkossa vasteena sille, että matkaviestin tukee mainittua toista matkaviestinverkkoa,

välitetään pyyntö ensimmäisestä matkaviestinverkosta mainittuun matkaviestimeen suorittaa mainitun toisen salausavaimen laskeminen ja

lasketaan mainitussa matkaviestimessä mainittu toinen salausavain vasteena mainitulle pyynnölle.

5. Patenttivaatimuksen 4 mukainen menetelmä, t u n n e t t u siitä, että

suoritetaan mainitun toisen salausavaimen laskeminen mainitussa ensimmäisessä matkaviestinverkossa vasteena sille, että matkaviestimen välittämä tunniste, kuten IMSI-tilaajatunniste, ja/tai classmark-tunniste ilmaisevat matkaviestimen tukevan mainittua toista matkaviestinverkkoa.

6. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

lasketaan mainittu toinen salausavain ensimmäisen matkaviestinverkon verkkoelementissä, kuten autentikaatiokeskuksessa, vasteena sille, että ensimmäisen matkaviestinverkon mainitun matkaviestimen välittämiä tunnisteita käsittävä verkkoelementti, kuten vierailijarekisteri tai kotirekisteri, pyytää toisen salausavaimen laskemista ja

välitetään mainittu toinen salausavain mainitusta salausavaimen laskevasta verkkoelementistä mainittuun matkaviestimen välittämiä tunnisteita käsittävään verkkoelementtiin.

7. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

mainittu matkaviestin käsittää tilaajan tunnistussovelluksen, kuten USIM-sovelluksen, mainittuun ensimmäiseen matkaviestinverkkoon ja tilaajan tunnistussovelluksen, kuten SIM-sovelluksen, mainittuun toiseen matkaviestinverkkoon,

välitetään matkaviestimen vastaanottamat toisen salausavaimen laskemiseen tarvittavat tiedot toisen matkaviestinjärjestelmän mukaiselle tunnistussovellukselle.

8. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

suoritetaan mainitun toisen salausavaimen laskeminen mainitussa ensimmäisessä matkaviestinverkossa ensimmäisen matkaviestinverkon mu-

kaisen autentikaatiovasteen ja ensimmäisen salausavaimen laskemisen yhteydessä,

välitetään ensimmäisen ja toisen salausavaimen laskemiseen tarvittavat tiedot, kuten satunnaislukuparametri, ensimmäisestä matkaviestinverkosta mainittuun matkaviestimeen,

välitetään matkaviestimessä mainitut ensimmäisen ja toisen salausavaimen laskemiseen tarvittavat tiedot ensimmäisen ja toisen matkaviestinverkon mukaiselle tunnistussovellukselle,

lasketaan toisen matkaviestinjärjestelmän mukaisessa tunnistussovelluksessa toinen salausavain ja ensimmäisen matkaviestinverkon mukaisessa tunnistussovelluksessa autentikaatiovaste,

välitetään mainittu ensimmäisen matkaviestinverkon mukainen autentikaatiovaste matkaviestimestä ensimmäiseen matkaviestinverkkoon ja

kuitataan matkaviestimen autentikaatio suoritetuksi toisen matkaviestinverkon osalta vasteena sille, että ensimmäinen matkaviestinverkko hyväksyy matkaviestimen välittämän autentikaatiovasteen.

9. Jonkin patenttivaatimuksen 1-7 mukainen menetelmä, t u n n e t t u siitä, että

suoritetaan toisen matkaviestinverkon mukaisen autentikaatiovasteen laskeminen ja satunnaislukuparametrin määrittäminen mainitun toisen salausavaimen laskemisen yhteydessä mainitussa ensimmäisessä matkaviestinverkossa,

välitetään pyyntö mainitulle matkaviestimelle suorittaa toisen matkaviestinverkon mukaisen autentikaatiovasteen laskeminen,

välitetään matkaviestimessä mainitun toisen salausavaimen laskemiseen tarvittavat tiedot toisen matkaviestinverkon mukaiselle tunnistussovellukselle,

lasketaan toisen matkaviestinverkon mukaisessa tunnistussovelluksessa toisen matkaviestinverkon mukaisen autentikaatiovaste toisensalausavaimen laskemisen yhteydessä,

välitetään matkaviestimessä laskettu toisen matkaviestinverkon mukainen autentikaatiovaste ensimmäiselle matkaviestinverkolle ja

tarkastetaan mainittu matkaviestimen välittämä toisen matkaviestinverkon mukainen autentikaatiovaste ensimmäisessä matkaviestinverkossa.

10. Jonkin patenttivaatimuksen 1-7 mukainen menetelmä, t u n n e t t u siitä, että

muutetaan mainittu ensimmäinen salausavain mainitun toisen salausavaimen mukaiseksi lyhentämällä ensimmäisessä matkaviestinverkossa ja mainitussa matkaviestimessä ennen yhteydensiirtoa toiseen matkaviestinverkkoon.

11. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

suoritetaan mainitun toisen salausavaimen laskeminen vasteena sille, että mainitussa ensimmäisessä matkaviestinverkossa päätetään tehdä handover toiseen matkaviestinverkkoon.

12. Tietoliikennejärjestelmä, joka käsittää ainakin ensimmäisen matkaviestinverkon, joka on järjestetty käyttämään ensimmäistä salausavainta matkaviestimen ja matkaviestinverkon välisen liikenteen salaamiseen, toisen matkaviestinverkon, joka on järjestetty käyttämään toista salausavainta matkaviestimen ja matkaviestinverkon välisen liikenteen salaamiseen, ja matkaviestimen, joita mainittuja erilaisia ensimmäistä ja toista matkaviestinverkkoa matkaviestin on järjestetty tukemaan, t u n n e t t u siitä, että

ensimmäinen matkaviestinverkko on järjestetty laskemaan mainittu toinen salausavain matkaviestimen toimiessa ensimmäisessä matkaviestinverkossa,

ensimmäinen matkaviestinverkko on järjestetty välittämään toisen salausavaimen laskemiseen tarvittavat tiedot ensimmäisestä matkaviestinverkosta mainittuun matkaviestimeen, kun matkaviestin toimii ensimmäisessä matkaviestinverkossa ja

matkaviestin on järjestetty laskemaan toinen salausavain.

13. Patenttivaatimuksen 12 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

mainittu matkaviestin ja mainittu toinen matkaviestinverkko on järjestetty salaamaan matkaviestimen ja toisen matkaviestinverkon välinen liikenne käyttäen mainittua toista salausavainta, jos matkaviestin siirtyy aktiivisen yhteyden aikana ensimmäisestä matkaviestinverkosta toiseen matkaviestinverkkoon.

14. Patenttivaatimuksen 12 tai 13 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

mainittu ensimmäinen matkaviestinverkko on järjestetty välittämään mainittu toinen salausavain mainittuun toiseen matkaviestinverkkoon ennen yhteydensiirtoa toiseen matkaviestinverkkoon,

mainittu matkaviestin on järjestetty välittämään mainittu matkaviestimessä laskettu toinen salausavain matkaviestimen salauksen suorittavalle välineelle vasteena sille, että ensimmäinen matkaviestinverkko välittää pyynnön matkaviestimelle yhteydensiirrosta toiseen matkaviestinverkkoon ja

matkaviestin ja toinen matkaviestinverkko on järjestetty käyttämään mainittua toista salausavainta liikenteen salaamiseen yhteydensiirron jälkeen.

15. Jonkin patenttivaatimuksen 12-14 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

mainittu ensimmäinen matkaviestinverkko on järjestetty tarkastamaan matkaviestimen välittämän tunnisteen, kuten IMSI ja/tai classmark-tunnisteen perusteella, tukeeko mainittu matkaviestin mainittua toista matkaviestinverkkoa,

ensimmäinen matkaviestinverkko on järjestetty laskemaan mainittu toinen salausavain vasteena sille, että matkaviestin tukee toista matkaviestinverkkoa,

ensimmäinen matkaviestinverkko on järjestetty välittämään pyyntö matkaviestimelle mainitun toisen salausavaimen laskemiseksi ja

matkaviestin on järjestetty laskemaan mainittu toinen salausavain mainitun pyynnön perusteella.

16. Jonkin patenttivaatimuksen 12-15 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

mainitun ensimmäisen matkaviestinverkon mainitun matkaviestimen välittämiä tunnisteita käsittävä verkkoelementti, kuten vierailijarekisteri tai kotirekisteri, on järjestetty välittämään pyyntö mainitun toisen salausavaimen laskemisesta ensimmäisen matkaviestinverkon verkkoelementille, kuten autentikaatiokeskukselle,

ensimmäisen matkaviestinverkon verkkoelementti, kuten autentikaatiokeskus, on järjestetty laskemaan mainittu toinen salausavain vasteena sille, että mainittu matkaviestimen välittämiä tunnisteita käsittävä verkkoelementti pyytää mainitun toisen salausavaimen laskemista ja

mainittu toisen salausavaimen laskeva verkkoelementti on järjestetty välittämään laskettu toinen salausavain mainittuun matkaviestimen välittämiä tunnisteita käsittävään verkkoelementtiin.

17. Jonkin patenttivaatimuksen 12-16 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

mainittu ensimmäinen matkaviestinverkko on järjestetty laskemaan mainittu toinen salausavain ensimmäisen matkaviestinverkon mukaisen autentikaatiovasteen ja ensimmäisen salausavaimen laskemisen yhteydessä,

ensimmäinen matkaviestinverkko on järjestetty välittämään ensimmäisen ja toisen salausavaimen laskemiseen tarvittavat tiedot, kuten satunnaislukuparametri, mainittuun matkaviestimeen,

matkaviestin käsittää ensimmäisen matkaviestinverkon mukaisen tunnistussovelluksen, kuten USIM-sovelluksen, ja toisen matkaviestinverkon mukaiselle tunnistussovellun, kuten SIM-sovelluksen,

matkaviestin on järjestetty välittämään mainitut ensimmäisen ja toisen salausavaimen laskemiseen tarvittavat tiedot ensimmäisen ja toisen matkaviestinverkon mukaiselle tunnistussovellukselle,

mainittu toisen matkaviestinverkon mukainen tunnistussovellus on järjestetty laskemaan mainittu toinen salausavain ja mainittu ensimmäisen matkaviestinverkon mukainen tunnistussovellus on järjestetty laskemaan ensimmäisen matkaviestinverkon mukainen autentikaatiovaste ja

matkaviestin on järjestetty välittämään ensimmäisen matkaviestinverkon mukainen autentikaatiovaste ensimmäiseen matkaviestinverkkoon.

18. Jonkin patenttivaatimuksen 12-16 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

mainittu ensimmäinen matkaviestinverkko on järjestetty suorittamaan mainitun toisen matkaviestinverkon mukaisen satunnaislukuparametrin määrittäminen ja autentikaatiovasteen laskeminen mainitun toisen salausavaimen laskemisen yhteydessä,

ensimmäinen matkaviestinverkko on järjestetty välittämään pyyntö mainittuun matkaviestimeen toisen matkaviestinverkon mukaisen autentikaatiovasteen laskemiseksi,

matkaviestin käsittää ensimmäisen matkaviestinverkon mukaisen tunnistussovelluksen, kuten USIM-sovelluksen, ja toisen matkaviestinverkon mukaiselle tunnistussovellun, kuten SIM-sovelluksen,

matkaviestin on järjestetty välittämään mainitun toisen salausavaimen laskemiseen tarvittavat tiedot toisen matkaviestinverkon mukaiselle tunnistussovellukselle,

mainittu toisen matkaviestinverkon mukainen tunnistussovellus on järjestetty laskemaan mainittu toinen salausavain ja toisen matkaviestinverkon mukaisen autentikaatiovaste olennaisesti samanaikaisesti,

matkaviestin on järjestetty välittämään toisen matkaviestinverkon mukainen autentikaatiovaste ensimmäiseen matkaviestinverkkoon ja

toinen matkaviestinverkko on järjestetty tarkastamaan toisen matkaviestinverkon mukainen autentikaatiovaste.

(57) Tiivistelmä

Menetelmä autentikaation ja salauksen järjestämiseksi tietoliikennejärjestelmässä, joka käsittää kaksi erilaista matkaviestinverkkoa, johon ensimmäiseen matkaviestinverkkoon matkaviestin on yhteydessä. Ensimmäisessä matkaviestinverkossa lasketaan toisen matkaviestinverkon mukainen salausavain ja välitetään salausavaimen laskemiseen tarvittavat tiedot matkaviestimelle, jossa lasketaan myös toisen matkaviestinverkon mukainen salausavain. Yhteyden siirryttyä toiseen matkaviestinverkkoon siirrytään salaamaan liikenne käyttämällä etukäteen laskettua mainittua salausavainta.
(Fig. 2)

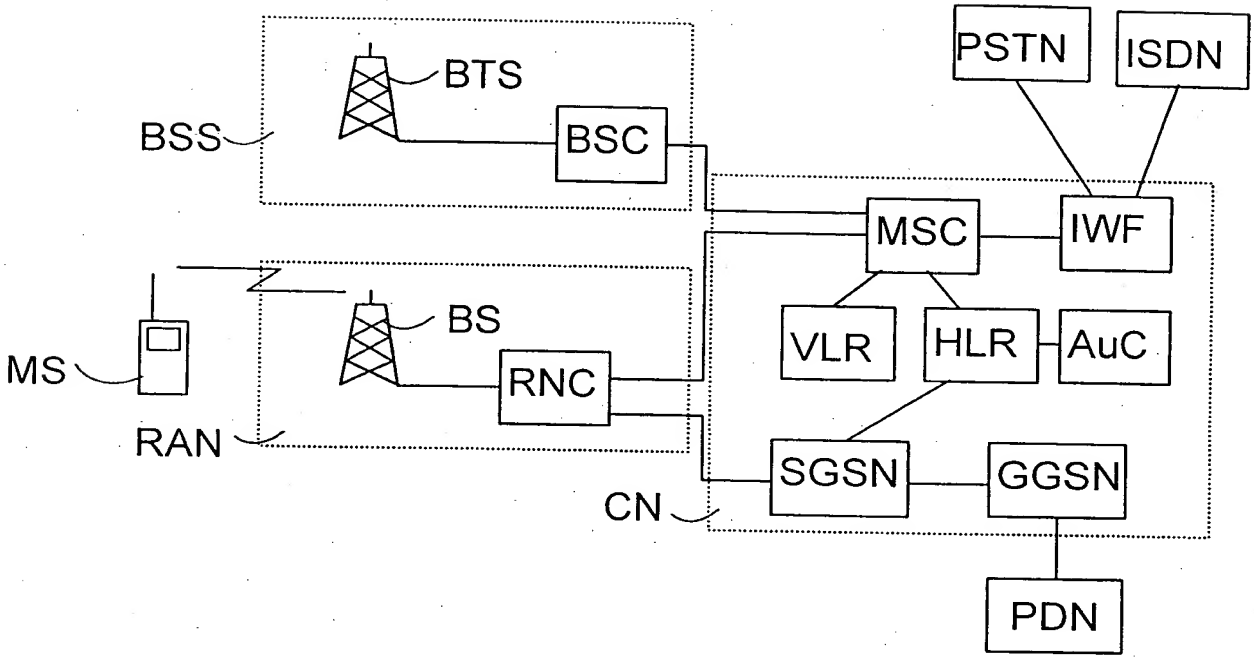
PSTN
ISDN
BTS
BSS
BSC
MSC
IWF
BS
MS
VLR
HLR
AuC
RNC
RAN
SGSN
GGSN
CN
PDN

Fig. 1

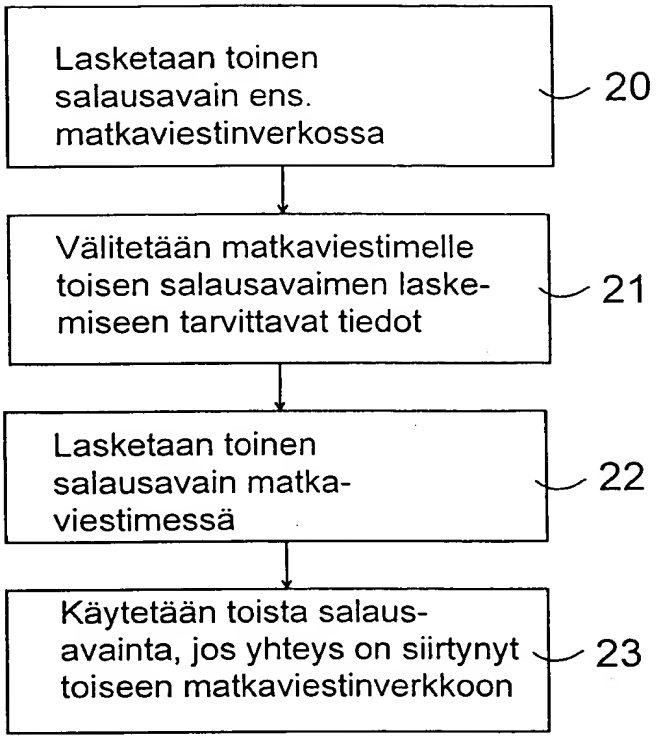
Lasketaan toinen salausavain ens. matkaviestinverkossa
20
Välitetään matkaviestimelle toisen salausavaimen laskemiseen tarvittavat tiedot
21
Lasketaan toinen salausavain matkaviestimessä
22
Käytetään toista salausavainta, jos yhteys on siirtynyt toiseen matkaviestinverkkoon
23

Fig. 2

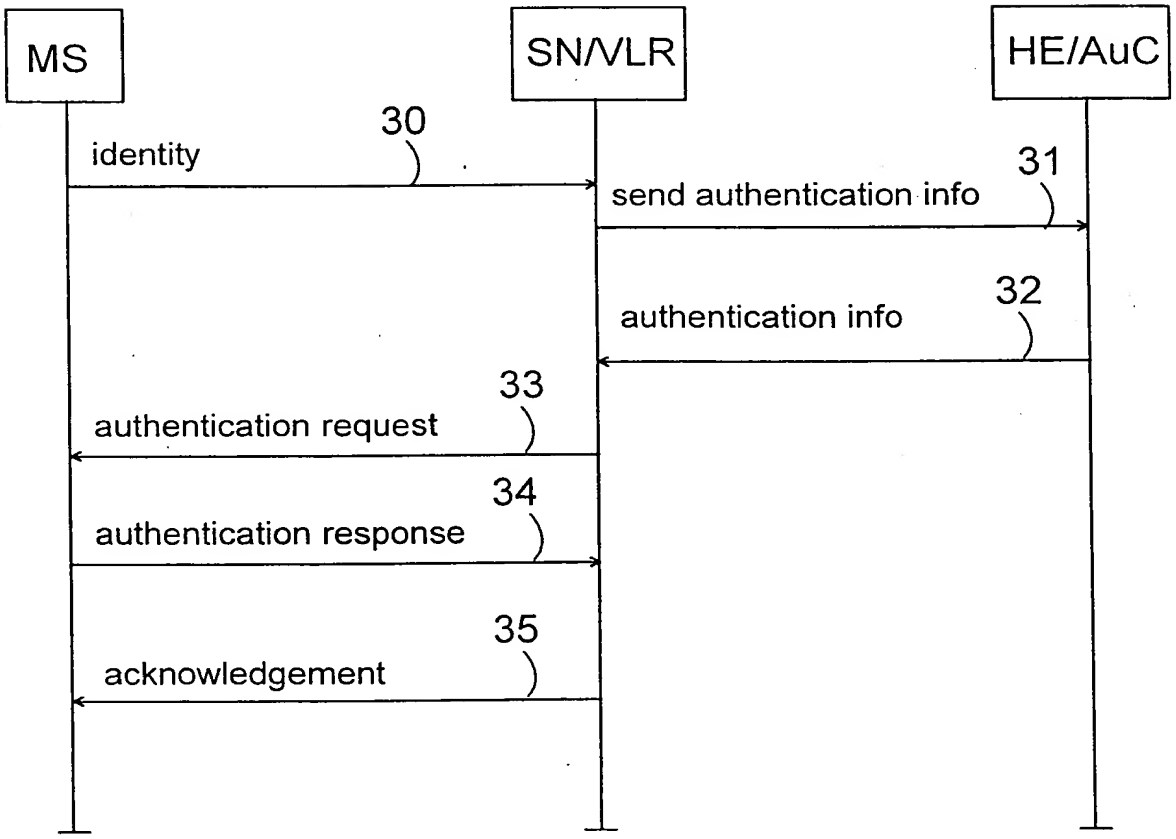
MS
SN/VLR
HE/AuC
30
identity
31
send authentication info
32
authentication info
33
authentication request
34
authentication response
35
acknowledgement

Fig. 3

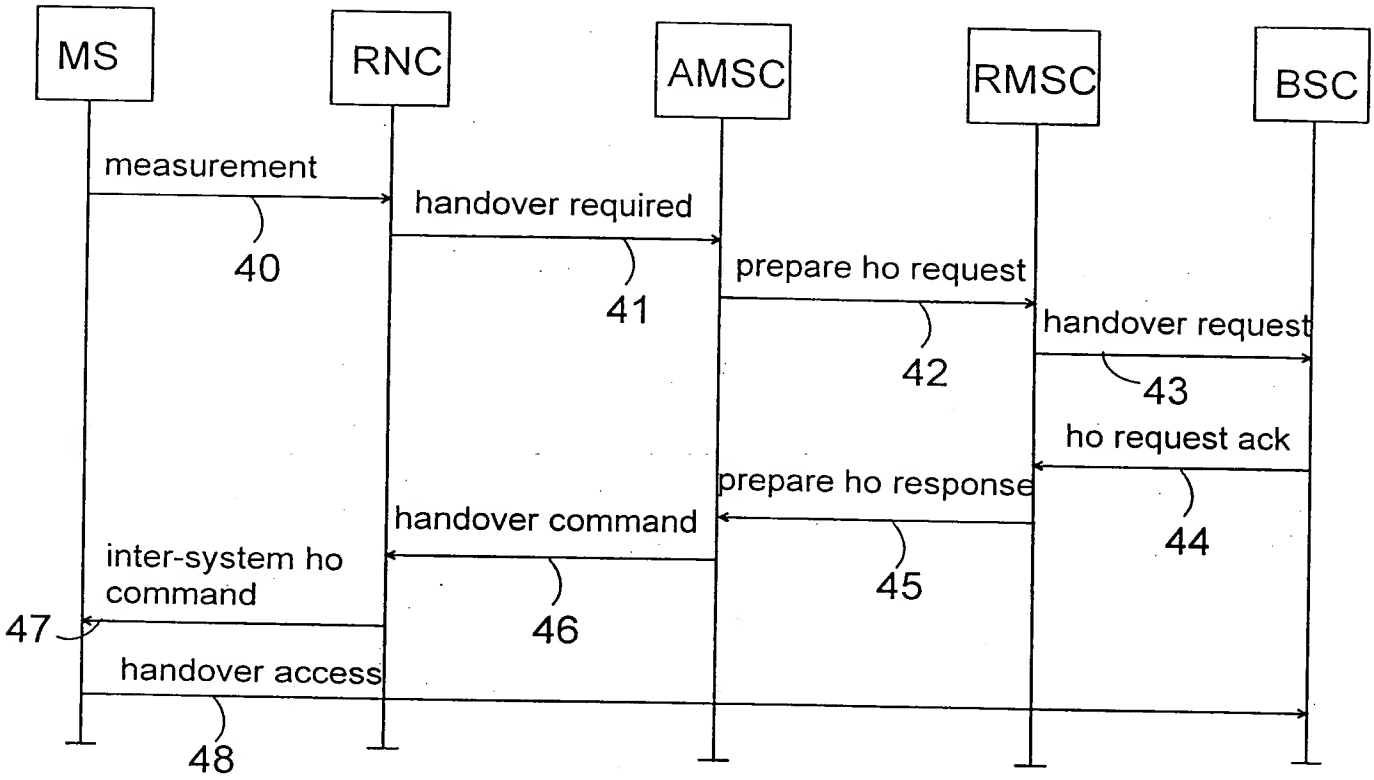
MS
RNC
AMSC
RMSC
BSC
measurement
40
handover required
41
prepare ho request
42
handover request
43
ho request ack
44
prepare ho response
45
handover command
46
inter-system ho command
47
handover access
48

Fig. 4